



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/737,372	12/16/2003	Glenn Gearhart	ACA1.PAU.02	5372
23386	7590	09/12/2007	EXAMINER	
MYERS DAWES ANDRAS & SHERMAN, LLP 19900 MACARTHUR BLVD., SUITE 1150 IRVINE, CA 92612			BAUM, RONALD	
ART UNIT		PAPER NUMBER		
2136				
MAIL DATE		DELIVERY MODE		
09/12/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/737,372	GEARHART, GLENN	
Examiner	Art Unit		
Ronald Baum	2136		

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 16 December 2003.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-7 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-7 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 16 December 2003 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 20031216.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
5) Notice of Informal Patent Application
6) Other: _____

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 16 December 2003.
2. Claims 1-7 are pending for examination.
3. Claims 1-7 are rejected.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1 and 2-7 (by dependency) are rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. The rejection under 35 U.S.C. 112, second paragraph, as being indefinite, as detailed below provides the analogous basis for the 35 U.S.C. 101 rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Appropriate correction is required.

Regarding claims 1 and 2-7 (by dependency), the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

The term(s) “can”, “can be”, “the *power*” and “may be” in claims 1 and 2-7 (by dependency) are relative term(s) that renders the claim indefinite. The term(s) “can”, “can be”, “the *power*” and “may be” are not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claims 1 and 2-7 (by dependency) are objected to because of the following informalities: the incorrect “.” after the phrase “recipient client”, and the “*a the* computer” are typographical errors requiring correction in claim 1, limitation “d)”, and “anywhere in the *worlds*” in claim 1, limitation “e)”.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-7 are rejected under 35 U.S.C. 102(b) as being anticipated by Jones et al, U.S. Patent No. 5,623,637.

7. As per claim 1; “An intelligent digital secure lock box and access key distribution system (DLB), comprising:

a) A source computer or digital device

which includes within the device

one or more digital lock boxes which

can be secured with encryption and within the lock boxes are one of more digital access codes or keys [*Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage (i.e., secure lock box) and encryption logic (i.e., digital lock boxes secured with encryption), and access controlled storage access to said storage contents (i.e., digital access codes or keys) via a programmable secret/cryptographic (i.e., PKI based) key, clearly encompasses the claimed limitations as broadly interpreted by the examiner.*];

b) One or more recipient clients

at receiving computers or digital devices which *can* receive one of more digital lock boxes and with a provided encryption access key to the delivered lock boxes such that the recipient client *can* obtain access to the contents of a delivered secure digital lock boxes [*Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage, encryption logic, and associated interfacing to configured digital devices (i.e., recipient clients of associated network) with access to said storage contents (i.e., digital access*

codes or keys) via a programmable secret/cryptographic (i.e., PKI based encryption access key) key, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

c) One or more removable storage devices (RSD) or digital media storage devices,

such as

a Flash USB drive,

a CD,

a DVD,

a computer diskette or

other media device,

can be used

to provide

optional programmability,

portability and

off-line storage, and

back-up storage capabilities

to one or more lock boxes [*Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage, encryption logic, and associated interfacing to configured digital devices with access to said storage contents of said smartcard that is in itself a removable storage device providing portability,*

programmability, etc., clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

d) Where the digital lock box

can be encrypted and

stored on

a the computer hard drive,

a removable digital storage media or

delivered digitally to

a designated distribution computer and

a ultimate recipient client [Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage, encryption logic, and associated interfacing to configured digital devices with access to said storage contents of said smartcard that is in itself a removable storage device providing portability, programmability, whereas the smartcard secured storage contents (i.e., digital lock box stored contents) are transferable to associated network components (i.e., delivered digitally to ultimate recipient client), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].

e) Where the digital lock box

can become

a personal item which the individual carries with him or her with

all of his or her secure access codes and passwords

allowing the individual
the *power* and *the capability to* quickly and easily
setup his access to e-mail accounts,
secure areas on web pages
open on-line banking and
other password or access key activities
from any computer anywhere in the *worlds* [Abstract, figures 1-3
and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the
detachable (i.e., personal item which the individual carries with him or
her) memory/smartcard with associated storage, encryption logic, and
associated interfacing to configured digital devices with access to said
storage contents of said smartcard that is in itself a removable storage
device providing portability, programmability, whereas the smartcard
secured storage contents (i.e., digital lock box stored contents, such as
electronic wallet/on-line banking oriented applications) are transferable
to associated network components (i.e., delivered digitally to ultimate
recipient client at any computer in the world), clearly encompasses the
claimed limitations as broadly interpreted by the examiner.].".

8. Claim 2 *additionally recites* the limitations that; "Wherein the contents of the digital lock box defined in claim 1 includes
digital access codes and

textual or digital imagery associated therewith.”.

The teachings of Jones et al (Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage, encryption logic, and associated interfacing to configured digital devices with access to said storage contents (i.e., digital access codes, keys, certificate/digital wallet information ‘textual or digital imagery’) via a programmable secret/cryptographic (i.e., PKI based encryption access key) key, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

9. Claim 3 *additionally recites* the limitations that; “Wherein the digital access codes defined in claim 1

can be manually and electronically generated:

encryption access keys,
pin numbers,
pass words,
account numbers,
ID numbers, and
associated types of
access codes and
sensitive, confidential or trade secret
codes or
ID data.”.

The teachings of Jones et al (Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage, encryption logic, and associated interfacing to configured digital devices with access to said storage contents (i.e., digital access codes, keys, certificate/digital wallet information ‘textual or digital imagery’, etc., is manually/electronically generated encryption access keys, confidential information per se) via a programmable secret/cryptographic (i.e., PKI based encryption access key) key, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

10. Claim 4 *additionally recites* the limitations that; “Wherein
the delivery of the encryption access key to
a delivered lock box defined in claim 1
can be by various means of delivery and
the delivered encryption access key
may open more than
just a single digital lock box.”.

The teachings of Jones et al (Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage, encryption logic, and associated interfacing to configured digital devices with access to said storage contents (i.e., digital access codes, keys, certificate/digital wallet information ‘textual or digital imagery’, etc., is manually/electronically generated/delivered encryption access keys, confidential information per se) via a programmable secret/cryptographic (i.e., PKI based encryption access key),

whereas the smartcard secured storage contents (i.e., digital lock box stored contents) are transferable to associated network components (i.e., delivered digitally to ultimate recipient client or clients across the network), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

11. Claim 5 *additionally recites* the limitations that; “Wherein the user of the lock box defined in claim 1 *has the capabilities*

to

input,

edit,

copy, and

delete

the digital access codes

stored in the digital lock box and

to

input,

edit,

copy, and

delete

the textual or digital imagery

associated therewith.”.

The teachings of Jones et al (Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage, encryption logic, and associated interfacing to configured digital devices with access to said storage contents (i.e., digital access codes, keys, certificate/digital wallet information ‘textual or digital imagery’, etc., is manually/electronically generated encryption access keys, confidential information per se) via a programmable secret/cryptographic (i.e., PKI based encryption access key) key, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

12. Claim 6 *additionally recites* the limitations that; “Wherein the user of the lock box defined in claim 1 *has the capabilities*
 - to use the device in
 - a stand alone,
 - single
 - computer or
 - digital device configuration or
 - as part of a configuration that includes
 - a network of
 - computers and
 - digital devices.”

The teachings of Jones et al (Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage, encryption logic,

and associated interfacing to configured digital devices with access to said storage contents (i.e., digital access codes, keys, certificate/digital wallet information ‘textual or digital imagery’, etc., is manually/electronically generated/delivered encryption access keys, confidential information per se) via a programmable secret/cryptographic (i.e., PKI based encryption access key), whereas the smartcard secured storage contents (i.e., digital lock box stored contents) are transferable to associated network components (i.e., delivered digitally to ultimate recipient client or clients across the network), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

13. Claim 7 *additionally recites* the limitations that; “Wherein the user of the lock box defined in claim 1 *has the capabilities*

to use the device in

a direct user present at

the computer or

digital device configuration or

as part of remote access configuration which

may include

wireline,

wireless or

other modes of communications.”.

The teachings of Jones et al (Abstract, figures 1-3 and associated descriptions, col. 1, lines 59-col. 2, line 58, whereas the detachable memory/smartcard with associated storage, encryption logic,

and associated interfacing to configured digital devices with access to said storage contents (i.e., *user* digital access codes, keys, certificate/digital wallet information 'textual or digital imagery', etc., is manually/electronically generated/delivered encryption access keys, confidential information per se) via a programmable secret/cryptographic (i.e., PKI based encryption access key) key, whereas the smartcard secured storage contents (i.e., digital lock box stored contents) are transferable to associated network components (i.e., delivered digitally to ultimate recipient client or clients remotely across the network), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

Conclusion

14. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


9/10/07

